Listing of Claims:

1. (Currently Amended) ~~An~~ A bit-level permutation apparatus comprising:

a plurality of switches each having a first input terminal, a second input terminal, a first output terminal and a second output terminal, each of the plurality of switches having a pass-through state in which data input to the first input terminal is passed to the first output terminal and data input to the second input terminal is passed to the second output terminal, and a cross-over state in which data input to the first input terminal is passed to the second output and data input to the second input terminal is passed to the first output terminal,

the plurality of switches interconnected to provide, at the output terminals of the plurality of switches, permutations of ~~signals~~ bits received via the input terminals of the plurality of switches

and wherein one or more of the plurality of switches has a broadcast state in which data input to one of the first input terminal and the second input terminal is passed to both the first output terminal and the second output terminal .

2. (Canceled).

3. (Original) The apparatus of claim 1 wherein the plurality of switches comprises 352 switches coupled as 32 by 11 array to provide a 64-bit Benes fabric.

4. (Original) The apparatus of claim 1 wherein one or more of the plurality of switches comprises:

a first multiplexer coupled to the first input terminal and to the second input terminal to receive signals from the first input terminal and the second input terminal, the first multiplexer to pass signals from the first input terminal and the second input terminal to the first output terminal; and

a second multiplexer coupled to the first input terminal and to the second input terminal to receive signals from the first input terminal and the second input terminal,

the second multiplexer to pass signals from the first input terminal and the second input terminal to the second output terminal.

5. (Original) The apparatus of claim 4 further comprising a control line to provide a control signal to the first multiplexer and to the second multiplexer such that when the control signal is in a first state the first multiplexer passes signals from the first input terminal to the first output terminal and the second multiplexer passes signals from the second input terminal to the second output terminal and when the control signal is in a second state the first multiplexer passes signals from the second input terminal to the first output terminal and the second multiplexer passes signals from the first input terminal to the second output terminal.

6. (Original) The apparatus of claim 1, wherein the plurality of switches are independently configurable.

7. (Original) The apparatus of claim 1 further comprising control circuitry coupled to the plurality of switches, the control circuitry to configure the plurality of switches.

8-11. (Canceled).

12. (New) A bit-level permutation method of encrypting a block of bits comprising the steps of:

obtaining a key comprising a series of bits;

obtaining a key schedule for permuting the key; and

permuting the key through a Benes switch fabric in accordance with the key schedule to form a permuted key.

13. (New) A method of encrypting a block of bits according to claim 12 and further comprising loading the key schedule into a control register coupled to the Benes switch fabric to effect said permuting the key.

14. (New) A method of encrypting a block of bits according to claim 12 wherein 16 subkeys are formed by partitioning the permuted key.

15. (New) A method of encrypting a block of bits according to claim 12 and further comprising:

partitioning the permuted key to form a plurality of subkeys;

circular-shifting each of the subkeys to form permuted subkeys; and

encrypting the block of bits using the permuted subkeys.

16. (New) A method of encrypting a block of bits according to claim 15 wherein said circular-shifting each of the subkeys includes circular-shifting at least one of the subkeys using a second Benes switch fabric.

17. (New) A method of encrypting a block of bits according to claim 15 wherein said circular-shifting each of the subkeys includes left circular-shifting at least one of the subkeys using a second Benes switch fabric.

18. (New) A method of encrypting a block of bits according to claim 15 wherein said circular-shifting each of the subkeys includes right circular-shifting at least one of the subkeys using a second Benes switch fabric.

19. (New) A method of encrypting a block of bits according to claim 15 wherein said circular-shifting each of the subkeys includes circular-shifting at least one of the subkeys a predetermined number of times using a second Benes switch fabric.

20. (New) A bit-level permutation method for encrypting a block of bits comprising the steps of:

obtaining a key comprising a series of bits;

obtaining a key schedule for permuting the key;

providing a modified Benes switch fabric comprising a plurality of 2-input switch elements in which at least one of the switch elements implements a pass state, a cross-over state, and a broadcast state;

permuting the key through the modified Benes switch fabric in accordance with the key schedule to form a permuted key; and

partitioning the permuted key to form a plurality of subkeys for encrypting the block of bits.

21. (New) A bit-level permutation method according to claim 20 wherein said permuting the key through the modified Benes switch fabric comprises a circular shift operation.

22. (New) A bit-level permutation method according to claim 20 wherein said permuting the key through the modified Benes switch fabric comprises an endian swap.

23. (New) A bit-level permutation method according to claim 20 wherein said permuting the key through the modified Benes switch fabric comprises a DES operation.